UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,114	01/16/2004	Shinsuke Suzuki	HITA.0495	4985

7590 11/23/2007

Stanley P. Fisher
Reed Smith LLP
Suite 1400
3110 Fairview Park Drive
Falls Church, VA 22042-4503

EXAMINER	
NAJEE-ULLAH, TARIQ S	
ART UNIT	PAPER NUMBER
4121	
MAIL DATE	DELIVERY MODE
11/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/758,114	SUZUKI ET AL.	
	Examiner	Art Unit	
	Tariq S. Najee-ullah	4121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/16/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/16/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is the first Office action in response to Application 10,758,114 filed on January 16, 2004. Claims 1-19 have been examined and are pending.

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on January 16, 2004 and October 29, 2007 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have been considered by the examiner.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant states, "*traffic control algorithms* based on *traffic control requests*" without specifying what

the requests are or where they originate. Applicant also fails to state the function or purpose of the algorithms. Applicant states, "sends the *traffic control algorithms* to said *traffic control interface*" without specifying the function of the algorithms as they relate to the interface.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by US Publication Number 2002/0162026 to Neuman et al (Neuman hereinafter).

Regarding claim 1, Neuman discloses **a traffic control computing device comprising: a traffic control interface to connect to traffic control devices which control traffic in a network** (Figure 1A, Page 1, paragraph [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor that handles all network communication, i.e. control traffic in a network.)**; a**

traffic control request interface to connect to traffic control request detecting devices which determine whether a traffic control must be executed by said traffic control devices (Fig. 3; Pg. 5, Par. [0071]; Neuman discloses the present invention, as illustrated in FIG. 3, places a secure, intelligent network interface, i.e. traffic control request interface, between the user workstation and the Internet and server, i.e. traffic control request detecting device, so as to provide firewall, i.e. traffic control device, features across all layers of the protocol stack, including filtering, i.e. determining whether a traffic control must be executed, based upon Distinguished Name or the authenticated universally unique username.); **a first storage device in which information about traffic control received via the traffic control request interface is stored** (Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control.); **a traffic control computing unit connected to said traffic control interface** (Fig. 1A, Pg. 1, par. [002]; Neuman discloses each node or computer on the

network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor, i.e. traffic control computing unit, that handles all network communication), **and connected to said traffic control request interface** (Pg. 1, par. [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control request interface, with a coprocessor, i.e. traffic control computing unit, that handles all network communication), **and connected to said first storage device, wherein said traffic control computing unit computes traffic control algorithms based on traffic control requests stored in the first storage device and sends the traffic control algorithms to said traffic control interface** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

Regarding claim 2, Neuman discloses **the traffic control computing device according to claim 1, further comprising: an information unit for acquiring information objects about traffic control details per a traffic control device associated with IDs of the traffic control devices which are now executed separately by said traffic control devices** (Pg. 1, par. [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor, i.e. an information unit, that handles all network communication. Pg. 3, par. [0046]; Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.)**; and second storage device in which said acquired information objects about traffic control details per traffic control device associated with the IDs of the traffic control devices are stored** (Pg. 4, par. [0069]; Neuman discloses all authentication information is stored on a Central Management Console (CMC) implying CMC also functions as a second storage device. Pg. 5, par. [0071]; Neuman discloses the present invention, places a secure, intelligent network interface between the user workstation and the Internet and server so as to provide firewall features across all layers of the protocol stack,

including filtering based upon Distinguished Name or the authenticated universally unique username, i.e. associated IDs of the traffic control devices.).

Regarding claim 3, Neuman discloses **the traffic control computing device according to claim 1, wherein IDs of said traffic control request detecting devices are stored in said first storage device** (Pg. 3, par. [0047]; Neuman discloses the invention allows transparent single sign on to any device, i.e. traffic control request detecting device, using applications or servlets supplied by the Central Management Counsel (CMC) to allow user/password, i.e. IDs, to be negotiated automatically. User/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.).

Regarding claim 4, Neuman discloses **the traffic control computing device according to claim 1, wherein said traffic control computing unit compares the sender of a traffic control request received through said traffic control request interface for a match with any of traffic control information objects stored in said first storage device** (Fig. 4 discloses the functions of the interface including

checks, user authentication, and response. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions. Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.) **and rejects said traffic control request if said sender of the received request is not stored in said first storage device** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control

request, is rejected since no access is granted unless the proper login information is stored on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been rejected by the CMC.).

Regarding claim 5, Neuman discloses **the traffic control computing device according to claim 4, further comprising a traffic control computing unit as a management interface which functions as a contact point for communicating with a network administrator** (Pg. 4, par. [0069]; Neuman discloses the interfaces of the present invention allow an administrator a single point of control, i.e. contact point, over all user access and user authentication information, including, but not limited to, passwords, user names, and any physical methods of identification via the Central Management Console (CMC).) **and is structured so that said traffic control computing unit checks whether a traffic control request that conflicts with said traffic control request received is included in said first storage device and** (Fig. 4, Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions. Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized

management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.), **if a conflicting traffic control request is included, compares the sender of the conflicting traffic control request with the sender of said traffic control request received, and, if both the senders are different, sends a notification of the conflicting requests to said traffic control computing management interface** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.).

Regarding claim 6, Neuman discloses **the traffic control computing device according to claim 5, wherein, if both said senders match, said traffic control computing unit is structured to assume that said sender of said conflicting traffic control request would have sent a**

request to cancel said conflicting traffic control request (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.).

Regarding claim 7, Neuman discloses **the traffic control computing device according to claim 2, wherein, when said information acquiring unit has been successful in acquiring a traffic control information object from a traffic control device, said traffic control computing unit is structured to determine that said traffic control device is operating and updates the traffic control information object for the traffic control device stored in said storage device to said traffic control information object newly acquired** (Pg. 3, par. [0043]; Neuman discloses memory can include updateable flash memory for the OS. An input is included for physical identification requirements, whether directly connected to the client machine, such as a serial, USB or parallel port, or

implemented as a port, such as a USB port or parallel port, on the secure, intelligent network interface.).

Regarding claim 8, Neuman discloses **the traffic control computing device according to claim 2, adapted so that when said traffic control information object has failed to be acquired from a traffic control device, said traffic control computing unit determines that said traffic control device is not operating and deletes the traffic control information object for the traffic control device determined as being non-operating from said storage device** (Fig. 9, Pg. 5, par. [0076; Neuman discloses the present invention provides non-host integrated fault tolerance. Fault tolerance is implemented between machines without needing to install any software or hardware on the critical machines. As illustrated in FIG. 9, by monitoring the server, i.e. traffic control device, from its network connection to ensure that it is still up or not, the secure, intelligent network interface can identify when functionality needs to be moved to the backup server. Although illustrated with respect to servers, it can be implemented on any machine, be it a workstation, mainframe, etc., that includes the interface of the present invention.).

Regarding claim 10, Neuman discloses **a traffic control method comprising: providing a traffic control computing device connected**

to traffic control devices which control traffic in a network and traffic control request detecting devices which detect what traffic control must be executed in the network (Fig. 3; Pg. 5, Par. [0071]; Neuman discloses the present invention, as illustrated in FIG. 3, places a secure, intelligent network interface, i.e. traffic control request interface, between the user workstation and the Internet and server, i.e. traffic control request detecting device, so as to provide firewall, i.e. traffic control device, features across all layers of the protocol stack, including filtering, i.e. determining whether a traffic control must be executed, based upon Distinguished Name or the authenticated universally unique username. Pg. 2, par. [0018]; Neuman discloses the invention will enable single sign-on, centralized password management, centralized security management, network auditing, intrusion detection (& prevention), web auditing and filtering, network arbitration, virus scanning, security vulnerability scanning, fault tolerance, machine diagnostics, encryption, authentication, firewalling, i.e. detect, key management, policy enforcement, and auditing.)**, receiving a traffic control request** (Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a

request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.); **storing the received traffic control request and the request sender information into a storage device** (Pg. 3, par. [0047]; Neuman discloses the invention allows transparent single sign on to any device, i.e. traffic control request detecting device, using applications or servlets supplied by the Central Management Counsel (CMC) to allow user/password, i.e. IDs, to be negotiated automatically. User/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.); **determining whether said received traffic control request conflicts with any of control requests previously stored in said storage device** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are

regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.); **and if no conflict is found, computing a control algorithm to complete said control request** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

Regarding claim 11, Neuman discloses **the traffic control method according to claim 10, further comprising: if said conflict exists, determining whether said sender of the received request and the sender of the conflicting control request match** (Fig. 4, Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions. Pg. 3, par. [0047];

Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients**; and if both the senders match, deleting said conflicting control request from said storage device** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. deleted, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is removed since no access is granted unless the proper login information is stored on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been deleted by the CMC.).

Regarding claim 12, Neuman discloses **the traffic control method according to claim 10, further comprising: if said conflict exists, determining whether said sender of the received request and the sender of the conflicting control request match** (Pg. 6, par. [0093]; Neuman discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.)**; if both the senders are different,**

notifying a network administrator that said conflict exists(Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable by an administrator. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server.)**;** **and resolving the conflict by decision made by the network administrator** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses a network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.)**.**

Regarding claim 13, Neuman discloses **the traffic control method according to claim 11, further comprising: determining whether the sender of the received traffic control request is from a pre-registered sender device** (Fig. 4, Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. Pg. 3, par. [0047]; Neuman discloses user/passwords

can be stored, i.e. pre-registered, on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of registration or saving on a storage device or medium that is part of the centralized management system.); **and rejecting the control request from a non-registered sender** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is rejected since no access is granted unless the proper login information is stored, i.e. pre-registered, on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been rejected by the CMC.).

Regarding claim 14, Neuman discloses **the traffic control method according to claim 13, wherein, if said sender of the received traffic control request is a pre-registered sender, said step of determining whether said received traffic control request conflicts with any of control requests previously stored in said storage device is executed** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e.

traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, i.e. the request is executed, or gives up.).

Regarding claim 15, Neuman discloses **the traffic control method according to claim 12, further comprising: receiving information as to whether said network administrator has rejected a part or all of either of the conflicting control requests** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server.)**; and notifying the sender of the rejected control request that the control request was rejected** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is rejected since no access is granted unless the proper login information

is stored, i.e. pre-registered, on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been rejected by the CMC.).

Regarding claim 16, Neuman discloses **the traffic control method according to claim 10, further comprising: comparing said computed control algorithm with control algorithms separately held by the traffic control devices connected to the computing device** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network.)**; if said computed control algorithm is not held by said traffic control devices, transmitting the computed control algorithm to the appropriate one of said traffic control devices** (Pg. 1, par. [0011]; Neuman discloses the secure, intelligent network interface can apply the appropriate encryption algorithm to the appropriate network device.).

Regarding claim 17, Neuman discloses **a network control method comprising: receiving a traffic control request** (Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request

to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.); **storing the received traffic control request and the request sender information into a storage device** (Pg. 3, par. [0047]; Neuman discloses the invention allows transparent single sign on to any device, i.e. traffic control request detecting device, using applications or servlets supplied by the Central Management Counsel (CMC) to allow user/password, i.e. IDs, to be negotiated automatically. User/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.); **determining whether said received traffic control request conflicts with any of control requests previously stored in said storage device** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master

repository on the CMC. These servlets translate the requests into manageable instructions.); **if no conflict is found, computing a control algorithm to complete said control request** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.); **and executing traffic control, according to the computed control algorithm** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the

central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

Regarding claim 18, Neuman discloses **a control method for a network comprising: providing traffic control devices which control traffic in the network, traffic control request detecting devices which detect what traffic control must be executed in the network, and a traffic control computing device which processes a traffic control request based on said detected traffic control requirement** (Fig. 3; Pg. 5, Par. [0071]; Neuman discloses the present invention, as illustrated in FIG. 3, places a secure, intelligent network interface, i.e. traffic control request interface, between the user workstation and the Internet and server, i.e. traffic control request detecting device, so as to provide firewall, i.e. traffic control device, features across all layers of the protocol stack, including filtering, i.e. determining whether a traffic control must be executed, based upon Distinguished Name or the authenticated universally unique username. Pg. 2, par. [0018]; Neuman discloses the invention will enable single sign-on, centralized password management, centralized security management, network auditing, intrusion detection (& prevention), web auditing and filtering, network arbitration,

virus scanning, security vulnerability scanning, fault tolerance, machine diagnostics, encryption, authentication, firewalling, i.e. detect, key management, policy enforcement, and auditing.)**,receiving, by said traffic control computing device, information (hereinafter referred to as first information) which comprises the identifiers of said traffic control request detecting devices, the detection functions of the traffic control traffic control request detecting devices, and traffic control requests which are now issued from the traffic control request detecting devices** (Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control. (Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control.)**; and storing the acquired first information into a storage device, wherein, upon**

receiving a new traffic control request from one of said traffic control request detecting devices, said traffic control computing device determines whether the newly received traffic control request conflicts with any of the traffic control requests stored in said storage device (Pg. 4, par. [0069]; Neuman discloses all authentication information is stored on a Central Management Console (CMC) implying CMC also functions as a second storage device. Pg. 5, par. [0071]; Neuman discloses the present invention, places a secure, intelligent network interface between the user workstation and the Internet and server so as to provide firewall features across all layers of the protocol stack, including filtering based upon Distinguished Name or the authenticated universally unique username, i.e. associated IDs of the traffic control devices.)**, if no conflict is found, calculates a control algorithm, based on the received traffic control request, and transmits the calculated control algorithm to the appropriate one of said traffic control devices** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further

discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions. Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

Regarding claim 19, Neuman discloses **the control method for the network according to claim 18, further comprising: acquiring second information which comprises the identifiers of said traffic control devices and the traffic control functions of the traffic control devices** (Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or

medium that is part of the centralized management system. Users and passwords are information associated with traffic control.); **and storing said second information acquired into the storage device** (Pg. 4, par. [0069]; Neuman discloses all authentication information is stored on a Central Management Console (CMC) implying CMC also functions as a second storage device. Pg. 5, par. [0071]; Neuman discloses the present invention, places a secure, intelligent network interface between the user workstation and the Internet and server so as to provide firewall features across all layers of the protocol stack, including filtering based upon Distinguished Name or the authenticated universally unique username, i.e. associated IDs of the traffic control devices.), **wherein, if the control algorithm calculated by said traffic control computing device has already been held by one of said traffic control devices, said traffic control computing device does not transmit the calculated control algorithm** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For

a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claim 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Neuman and further in view of Minear et. al US Patent 5,983,350 (Minear hereinafter).

Regarding claim 9, Neuman discloses **a traffic control computing device comprising: a traffic control interface to connect to traffic control devices which control traffic in a network** (Figure 1A, Page 1, paragraph [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor that handles all network communication, i.e. control traffic in a network.)**; a traffic control request interface to connect to traffic control request detecting devices which determine what traffic control must be executed by said traffic control devices** (Pg. 1, par. [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control request interface, with a coprocessor, i.e. an information unit, that handles all network communication. Fig. 3; Pg. 5, Par. [0071]; Neuman discloses the present invention, as illustrated in FIG. 3, places a secure, intelligent network interface, i.e. traffic control request interface, between the user workstation and the Internet and server, i.e. traffic control request detecting device, so as to provide firewall, i.e. traffic control device, features across all layers of the protocol stack, including filtering, i.e. determining whether a traffic control must be executed, based upon Distinguished Name or the authenticated

universally unique username.); **a traffic control request list containing information objects about traffic control received through the traffic control request interface associated with IDs of the traffic control request detecting devices which sent the information objects** (Pg. 3, par. [0046]; Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.); **a list of traffic control request detecting devices containing the IDs and functions of the traffic control request detecting devices connected to said traffic control computing device** (Pg. 3, par. [0046]; Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.); **a list of traffic control devices containing the IDs and functions of the traffic control device connected to said traffic control computing device** (Pg. 3, par. [0046]; Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.); **a traffic control method list containing the IDs of the connected traffic control devices and control details which are now executed by the traffic control devices** (Pg. 3, par. [0046];

Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.**); and a traffic control computing unit which computes control algorithms, based on control requests described in said traffic control request list** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.**).**

While Neuman discloses **a traffic control computing device comprising: a traffic control interface to connect to traffic control devices which control traffic in a network; a traffic control request interface to connect to traffic control request detecting devices which determine what traffic control must be executed by said traffic control devices; a traffic control request list containing information objects about traffic control received through the traffic**

control request interface associated with IDs of the traffic control request detecting devices which sent the information objects; a list of traffic control request detecting devices containing the IDs and functions of the traffic control request detecting devices connected to said traffic control computing device; a list of traffic control devices containing the IDs and functions of the traffic control device connected to said traffic control computing device; a traffic control method list containing the IDs of the connected traffic control devices and control details which are now executed by the traffic control devices; and a traffic control computing unit which computes control algorithms, based on control requests described in said traffic control request list, he does not explicitly express a "list" containing IDs of the connected traffic control devices.

Minear discloses "list" by disclosing a Security Association Database, i.e. list, stored within the firewall that contains identification information (Column 4, lines 59-67).

Neuman and Minear are analogous art because they are from the same field of endeavor of secure network communication. They are also found in the same US Patent Classification and Subclass.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to use Minear's security association database modification in Neuman's method.

The suggestion/motivation would have been to provide a system and method for securely transferring information between firewalls over an unprotected network (Col. 1, lines 8-25).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent Number 5,968,176 to Nessett et al titled "Multilayer Firewall System."
- US Publication Number 2006/0020688 to Chang et al relating to Client-Server network computing involving firewalls, gateways, and security policies.
- US Publication Number to 2002/0069278 to Forslow relating to Security Solutions for Virtual Private Networks.
- US Publication Number 2002/0059451 to Haviv relating to Client-Server network communication involving firewalls, gateways, network security policies, and authentication.

- US Patent Number 6,519,636 to Engel et al titled "Efficient classification, manipulation, and control of network transmissions by associating network flows with rule based functions."
- US Patent Number 6,463,474 to Fuh et al titled "Local authentication of a client at a network device".
- US Patent Number 6,219,706 to Fan et al titled "Access control for networks".
- US Patent Number 6,212,558 to Antur et al titled "Method and apparatus for configuring and managing firewalls and security devices".
- US Patent Number 6,052,788 to Wesinger et al titled "Firewall providing enhanced network security and user transparency".
- US Patent Number 6,006,259 to Adelman et al titled "Method and apparatus for an internet protocol (IP) network clustering system".
- US Patent Number 5,983,350 to Minear et al titled "Secure Firewall Supporting Different Levels of Authentication Based on Address or Encryption Status."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tariq S. Najee-ullah whose telephone number is (571) 270-5013. The examiner can normally be reached on Monday through Friday 8:00 - 5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TN

George Neurauter
Primary Examiner